Amendments to the Claims

Claim 1 (currently amended): A computer-implemented method of providing cross-domain authentication in a computing environment, comprising steps of:

providing security credentials of an entity to an initial point of contact that provides content aggregation in the computing environment;

passing the provided credentials from the initial point of contact to a trust proxy;

authenticating the passed credentials with an authentication service in a local security domain of the trust proxy to authenticate the entity for accessing content from at least one local content service, each of the at least one local content services operable to provide its content from the local security domain for aggregation, by the initial point of contact, in an aggregated view; and

using the authentication performed by the local authentication service to seamlessly authenticate the entity for accessing other content from at least one remote content service in each of [[to]] at least one ~~or more~~ selected remote security domains, each of the at least one remote content services operable to provide its content from its remote security domain for aggregation, by the initial point of contact, in the aggregated view. ~~domains.~~

Claim 2 (currently amended): The method according to Claim 1, [[when]] wherein the using step further comprises the steps of:

consulting policy information to determine which of a plurality of remote security domains should be selected as the at least one remote security domain; ~~to receive information from the local authentication service;~~ and

passing the information from the local authentication service to each of the determined remote security domains.

Claim 3 (currently amended): The method according to Claim 1, wherein the using step enables each of the remote content services in the selected remote security domains to be accessed by the entity without requiring the entity to provide its security credentials for those remote content services.

Claim 4 (currently amended): The method according to Claim 3, wherein a credential mapping operation is performed to map the provided security credentials to the entity's security credentials for each remote content service.

Claim 5 (original): The method according to Claim 1, wherein the entity is an end user.

Claim 6 (original): The method according to Claim 1, wherein the initial point of contact is a portal interface.

Claim 7 (original): The method according to Claim 1, wherein the passing step is performed by a proxy of the initial point of contact.

Claim 8 (original): The method according to Claim 7, wherein the proxy of the initial point of contact performs a protocol conversion, when passing the provided credentials, from a first

protocol used in the providing step to a second protocol used by the trust proxy.

Claim 9 (original): The method according to Claim 8, wherein the first protocol is Hypertext Transfer Protocol ("HTTP") or a security-enhanced version thereof.

Claim 10 (original): The method according to Claim 8, wherein the second protocol is Simple Object Access Protocol ("SOAP").

Claim 11 (canceled)

Claim 12 (original): The method according to Claim 1, wherein the using step further comprises the steps of:

forwarding a security token from the local authentication service to a remote trust proxy in each of the selected remote security domains; and

using the forwarded security token, at each of the remote trust proxies, to authenticate the entity with an authentication service in the remote security domain.

Claim 13 (original): The method according to Claim 12, wherein results of the authentication by the authentication service in the local security domain and results of each authentication by the authentication services in each selected remote security domain are returned to the initial point of contact.

Claim 14 (currently amended): The method according to Claim 13, further comprising the step of determining, by the initial point of contact, which of the content and the other content ~~services and/or views thereof~~ can be ~~provided to the entity~~ aggregated by the initial point of contact based on the returned results.

Claim 15 (original): The method according to Claim 1, wherein the entity has security credentials, in at least one of the selected remote security domains, that differ from the provided security credentials, and wherein the using step transparently maps the provided security credentials to the different security credentials.

Claim 16 (currently amended): A system for enabling an entity to have seamless access to a plurality of aggregated services which have different identity requirements, comprising:

means for initially authenticating the entity, by a first authentication component, for access to a first service using an identity provided by the entity;

means for mapping the provided identification to the differing identity requirements of at least one other service to be aggregated with the first service, thereby establishing mapped identity requirements for each of the at least one other services;

means for subsequently authenticating the entity for access to each of the at least one other services, by an authentication component associated with ~~each of the at least one services~~ that other service, using the mapped identity requirements; and

means for aggregating each of the at least one other services and the first service ~~a service associated with the initial authentication component~~, if the authentications thereof are successful,

into an aggregated result.

Claim 17 (original): The system according to Claim 16, wherein the aggregated result is an aggregated view.

Claim 18 (original): The system according to Claim 16, wherein the entity is a programmatic entity.

Claim 19 (currently amended): A computer program product for providing federated identity management within a distributed content aggregation framework, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code [[means]] for providing, to the content aggregation framework by a using entity, initial identity information that identifies the using entity for accessing a first content source that is operable within a first security domain;

computer-readable program code [[means]] for authenticating the initial identity information by a first authentication service in [[a]] the first security domain;

computer-readable program code [[means]] for conveying results of the authentication by the first authentication service to at least one ~~or more~~ selected other authentication ~~services~~ service, each of which is associated with ~~one or more other~~ a remote security ~~domains~~ domain that is distinct from the first security domain; [[and]]

computer-readable program code [[means]] for using the conveyed results to authenticate the using entity to each of the selected other authentication services for accessing a remote

content source operable within the remote security domain that is associated with that selected other authentication service, without requiring the using entity to provide additional identity information; and

aggregating content from the first content source and other content from each of the remote content sources for presentation in an aggregated view rendered by the content aggregation framework.

Claim 20 (original): The computer program product according to Claim 19, wherein the initial identity information is a name and password associated with the using entity.

Claim 21 (new): The method according to Claim 1, further comprising the step of rendering, by the initial point of contact, the aggregated view.